Approved by Committee on 1 September 2025

Information Governance Committee
Monday 12 May 2025 at 9.30am
Meeting Room 1, Eglinton House, Ailsa campus

Present: Mr Marc Mazzucco, Non-Executive Board Member (Chair)
Ms Sheila Cowan, Non-Executive Board Member (Vice Chair)
Mrs Jean Ford, Non-Executive Board Member
Mrs Sharon Morrow, Non-Executive Board Member

Ex-officio: Mrs Lesley Bowie, Board Chair
Ms Claire Burden, Chief Executive and Senior Information Risk Owner
Mrs Nicola Graham, Director of Infrastructure and Support Services
Ms Marie Lynch, Interim Head of Information Governance and Data Protection Officer
Dr Crawford McGuffie, Medical Director and Caldicott Guardian

In attendance: Mr Martin Duggan, Cyber Security Manager item 6.1
Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Apologies for absence

1.1 Apologies were noted from Cllr Douglas Reid.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 24 February 2025

The minute of the meeting held on 24 February 2025 was approved as an accurate record of the discussion, subject to the following change being made:

Item 6.1, Cyber Security update, fourth paragraph – Mr Duggan clarified in reply to a query from a member on the BC/DR exercise schedule 2025-2027 that it was correct that the same ransomware table-top exercise was planned annually as this was currently the highest cyber security risk to any organisation.

4. Matters Arising

4.1 The action log had previously been circulated to Committee members and all progress against actions was noted.

Committee members received an update on the following actions:

I**tem 7.3 (24/02/25), Information Governance Operational Delivery Group** – NHS Dumfries & Galloway cyber security presentation to

Area Clinical Forum circulated to IGC and IGODG members for awareness. Action complete.

Item 6.2.4 (11/11/24), FOI update – The Medical Director, Dr Crawford McGuffie, advised that there had not yet been a meeting with MPs and MSPs and this would be on the agenda for the next meeting. The Chief Executive advised that in the meantime she was taking the opportunity to raise the issue at one-to-one meetings with MPs and MSPs. Members noted that other Board areas were experiencing a similar position in terms of the volume of FOI requests. Action complete.

Item 6.2.4 (29/04/24), ICO audit report action plan – Action A04 ongoing. As previously advised, there were plans to complete action A06 by 31 August 2025 to enable submission of the Controlled Document policy to IGC meeting on 1 September 2025. Ongoing.

All other matters arising were either on the agenda, a date had been scheduled for the discussion or the action was complete.

4.2 **IGC Work Plan 2025** – Committee members noted the work plan.

5. Risk

5.1 Information Governance Strategic Risk Register

The Medical Director, Dr Crawford McGuffie, presented the Risk Register report.

The Director advised that the two risks assigned to IGC had been reviewed during the reporting period, with no change to the risk grading for either of these risks.

Risk ID 557 (Information Governance) – additional control measures had been added during the reporting period. The risk would be further refined prior to the next meeting to describe control measures with timescales.

Risk ID 603 (Cyber incident) had been carefully reviewed and updated to reflect the Network and Information Systems (NIS) audit which showed continuing improvement, with a score of 96%. However, the risk remained high and was unlikely to reduce due to new threats appearing on a daily basis across the UK public and private sector.

There were no proposed risks for escalation or termination.

Committee members discussed and scrutinised the two IGC risks specifically in relation to likelihood and consequence scores. For Risk ID 557 (Information Governance), members considered if the likelihood should be reduced given the additional control measures put in place. For Risk ID 603 (Cyber incident), members considered if the likelihood score was too low given that threats

changed on a daily basis. Members noted that a short life working group (SLWG) on risk was being set up which would inform future risk reporting. The Chief Executive assured members that for areas of sustained risk, the Board committed to review these risks more regularly, including the control measures in place to maintain the risk at an acceptable level.

Dr McGuffie underlined the continuous improvement approach being adopted by the Risk team to further improve the risk management process. Consideration would be given to potential and target scores for both IGC risks and an update provided at the next Committee meeting. **CMcG/NG**

Outcome: Committee members noted the report and took assurance from work being done to manage strategic risks which fall under the committee's governance remit.

5.2 There were no risk issues to report to the Risk and Resilience Scrutiny and Assurance Group.

6. Information Governance

6.1.1 Cyber Security update

The Director of Infrastructure and Support Services, Nicola Graham, introduced and invited Martin Duggan, Cyber Security Manager, to present the assurance report on the activities of the Cyber Security team. The report was provided in a new format following feedback from the Committee.

Martin Duggan highlighted the following key areas of activity:

- NHSAA had made strong progress in improving its cyber security. Board achieved 96% compliance with the Network and Information Systems (NIS) audit, an uplift of 9% compared to last year.
- A business continuity and disaster recovery exercise had taken place in December 2024 and further exercises were planned over the next three years.
- The Board had reduced by half the number of known cyber weakness over the last year. There were no significant issues to highlight in relation to antivirus activity. Members requested that future reports provide detail of tolerance levels in relation to antivirus activity to enable members to monitor the position. **NG/MD**
- Data indicated that around 30% of staff had not yet undertaken Cyber security training introduced in October 2023. However, system issues due to Learnpro and Turas systems not being linked in summer 2024 may have resulted in some under-reporting of training compliance. Communication was planned to encourage staff to complete this training.
- Members received a summary of incidents closed by the team during the last quarter. During this period there were

vulnerabilities identified related to VPN. Software had been upgraded and the position had improved. The Director confirmed in reply to a question from a member that future reports would provide the completion rate for incidents to give context.

- Audit Scotland external audit was ongoing and evidence had been provided from NIS audit in relation to cyber resilience. An Internal audit was planned for October 2025, with the scope of the audit to be agreed closer to the audit.
- The report outlined ongoing projects and improvement work, including focused work to support cyber security through CyberScotland Week 2025; team development and certification; cyber upskilling fund; phishing simulation; Cylera IOT management; and password policy.

Members discussed the report and supported the new format and information provided.

The Director advised in reply to a question from a member that the team would link in with the Engagement team to consider how to effectively communicate to staff how to manage suspicious email activity.

6.1.2 **NIS Audit update**

Committee members received a detailed update on the NIS audit 2024/25, the second year of a three year audit cycle. The Board had achieved 96% compliance, an increase of 9% compared to last year, with 93% of all controls achieved. The report provided details of progress against key performance indicators (KPI). NHSAA had achieved the advanced 90-90-0 KPI, a significant achievement. There were no categories or sub-categories that achieved below 60%. Auditor feedback demonstrated that NHSAA was a high performing Board in this area.

Mr Duggan advised that while the overall position was positive, there were areas which required further development. He highlighted an area of ongoing risk related to supplier management and mitigating actions. The Director gave assurance that supplier and contract management were priority areas to be taken forward by the new Assistant Director, Digital Services, once in post. The Committee would receive an update on progress at a future meeting, with exception reporting as required going forward.

Members commended the team for the good performance achieved and progress made. It was acknowledged that while the NIS audit reported good progress in relation to the controls in place, it did not demonstrate how effectively the Board was managing areas of risk.

Outcome: **Committee members noted the summary of the Cyber Security team's activities over the reporting period. Members commended the team for the significant progress made with the NIS audit.**

6.2 **Information Governance Update report**

The interim Head of IG and DPO, Marie Lynch, presented the combined Information Governance update and the following areas were highlighted:

6.2.1 **Information Security Incident Report** – The report covered the period January to March 2025. There were 20 information security breaches reported during this period, lower than the quarterly average of 25 breaches, based on data over the last three years.

There were no personal breaches considered notifiable to the Information Commissioner's Office (ICO) and ICO did not receive any complaints related to NHSAA's processing of personal data. The majority of incidents were categorised as Caldicott, Confidentiality and Data Protection and involved data being inadvertently emailed or given to the wrong people, similar to previous reports. The highest number of incidents reported were in Acute and the Health and Social Care Partnerships although this is expected due to their size and the nature of information processed.

Following discussion at the last Committee meeting, Ms Lynch had reached out to IG Leads for similar sized Boards. NHS Tayside and NHS Lanarkshire had provided comparison data which showed that there were significantly less breaches in NHSAA compared to these areas although the reason for this was unclear. It was noted that as a counterbalance patients and the public could make a complaint directly to the ICO and, as stated above, they had not received any complaints related to security breaches in NHSAA. Ms Lynch advised in reply to a question from a member that as ICO did not publish the number of breaches reported to them it was difficult to benchmark against other Board areas.

6.2.2 **Record of Processing Activity (ROPA) –** Marie Lynch outlined the background to NHSAA adopting OneTrust as a ROPA following a Once for Scotland approach. The national OneTrust contract had now ended and Boards had been asked if they would like to adopt a new platform which would incur costs for participating Boards. A number of Boards had chosen not to adopt the new platform. There would be no cost for Boards who chose not to use the new national platform. Following discussion at the Information Governance Operational Delivery Group, NHSAA was considering whether M365 could provide functionality as part of its implementation.

Committee members commended the team for the agile approach to extract information from OneTrust before the national contract ended which should enable rapid transfer to M365 once a solution has been identified, taking on board learning from other Board areas. Members received assurance that the Board was in compliance with article 30 obligations as only the ROPA was statutory.

6.2.3 **IG work programme 2024/25 –** Members received an update on the work programme in the following areas:

Public Records (Scotland) Act 2011:

- Element 4, business classification scheme – NHSAA had adopted the national scheme to be implemented as part of Sharepoint implementation with 31 March 2027 target completion date.
- Element 6, destruction arrangements – actions related to this were covered in the directorate's corporate records management improvement plans, with progress monitored through the Corporate Management Team. There were already robust procedures in place for destruction of health records.
- Element 11, audit trail – this action was on track and awaited Sharepoint implementation by 31 March 2027.
- Element 15 contract clause – this was included in generic terms and conditions for goods and services. Discussion was ongoing with service level agreement (SLA) team about how to incorporate into SLAs. Engagement was ongoing with Procurement and DPOs to include in contract variation notice.

Freedom of Information:

- The new IG Assurance Officer and new IG Analyst had completed this training. Action complete.

M365:

- The local IG team continued to support M365 implementation and completion of data protection impact assessment. The action related to Acceptable User Standards was ongoing. Members requested that target completion dates be changed to ongoing where the target date was not known. **ML**

ICO audit action A04:

- As reported under matters arising, the Controlled Document Policy was still under review with a target completion date of 31 August 2025.

6.2.4 **Information Commissioner's Office audit action plan**

An update was provided at item 8.2.3 above.

Outcome: Members noted the IG report and took assurance from the work being done to promote compliance with the relevant legislative frameworks.

7. Corporate Governance

7.1 Information Governance Committee Annual Report 2024/25

The interim Head of IG and DPO, Ms Marie Lynch, presented the Committee's 2024/25 annual report, including a self-assessment checklist, assurance mapping report and assurance reporting to NHS

Board. The report provided assurance that the Committee had fulfilled its remit during the year.

This had been another challenging year for the team due to workforce and workload pressures and it was hoped that the position would improve in 2025/26. The team had employed an IG Assurance Officer in September 2024 and the role had supported Freedom of Information and corporate records management activity. The team had managed to maintain high compliance across all areas of information governance and to build strong relationships across the Board. The Chair commended the team for delivering their role to a high standard, often under challenging circumstances.

Outcome: Committee members approved the Committee's annual report for onward submission to the NHS Board.

7.2 **Information Governance Operational Delivery Group** – there were no minutes to report.

8. Key issues to report to NHS Board

8.1 Committee members agreed that the following key issues be reported to the NHS Board meeting on 2 June 2025:

- Strategic risk register – IGC risks
- Cyber security/NIS audit update
- IG – ROPA update
- IGC annual report approved for onward submission to NHS Board.

9. Any Other Competent Business

9.1 There was no other business.

10. Date and Time of Next Meeting

Monday 1 September 2025 at 9.30am, MS Teams meeting

Approved by the Chair, Marc Mazzucco Date: 1 September 2025